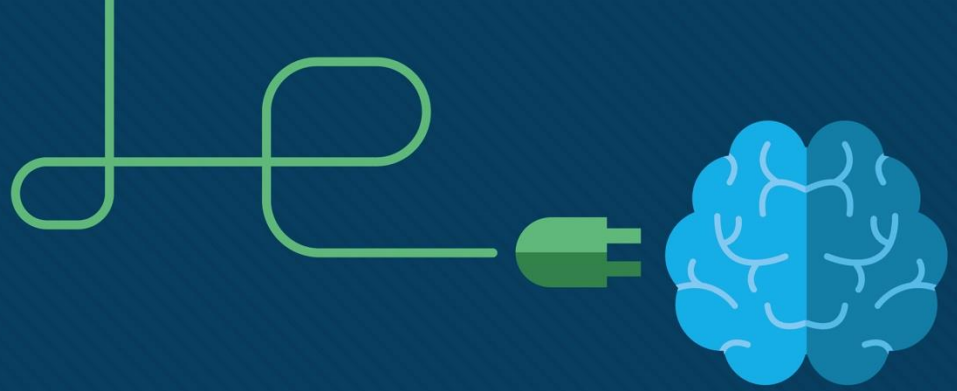


Modül 16: Ağ Güvenliği Temelleri

Ağlara Giriş v7.0 (ITN)

Modül Hedefleri

Modül Başlığı: Ağ Güvenliği Temelleri

Modül Amacı: Güvenliği artırmak için aygıt güçlendirme özellikleriyle anahtarları ve yönlendiricileri yapılandırma

Konu Başlığı	Amaç
Güvenlik Tehditleri ve Açıkları	Ağ cihazlarında neden temel güvenlik önlemlerinin gerekli olduğunu açıklama
Ağ Saldırıları	Güvenlik açıklarını belirleme
Ağ Saldırılarını Azaltma	Genel azaltma tekniklerini tanımlama
Cihaz Güvenliği	Güvenlik tehditlerini azaltmak için ağ aygıtlarını aygıt güçlendirme özellikleriyle yapılandırma

16.1 Güvenlik Tehditleri ve Açıkları

Tehdit Türleri

Bir ağa yapılan saldırılar yıkıcı olabilir ve önemli bilgi veya varlıkların hasar görmesi veya çalınması nedeniyle zaman ve para kaybına neden olabilir. İzinsiz girenler, yazılım güvenlik açıkları, donanım saldırıları veya birinin kullanıcı adı ve şifresini tahmin ederek bir ağa erişim sağlayabilir. Yazılımı değiştirerek veya yazılım güvenlik açıklarını kullanarak erişim elde eden davetsiz misafirlere tehdit aktörleri denir.

Tehdit aktörü ağa erişim kazandıktan sonra, dört tür tehdit ortaya çıkabilir:

- Bilgi Hırsızlığı
- Veri Kaybı ve manipülasyonu
- Kimlik Hırsızı
- Hizmet Kesintisi

Açık Türleri

Güvenlik açığı, bir ağ veya cihazdaki zayıflık derecesidir. Yönlendiriciler, anahtarlar, masaüstleri, sunucular ve hatta güvenlik cihazlarında bir dereceye kadar güvenlik açığı vardır. Tipik olarak, saldırı altındaki ağ cihazları, sunucular ve masaüstü bilgisayarlar gibi uç noktalardır.

Üç temel güvenlik açığı veya zayıflık vardır:

- Teknolojik Güvenlik Açıkları arasında TCP / IP Protokolü zayıflıkları, İşletim Sistemi Zayıflıkları ve Ağ Ekipmanı zayıflıkları yer alabilir.
- Yapılandırma Açıkları, güvenli olmayan kullanıcı hesaplarını, kolayca tahmin edilebilen şifreli sistem hesaplarını, yanlış yapılandırılmış internet hizmetlerini, güvenli olmayan varsayılan ayarları ve yanlış yapılandırılmış ağ ekipmanını içerebilir.
- Güvenlik Politikası Güvenlik açıkları, yazılı bir güvenlik politikasının eksikliğini, politikayı, kimlik doğrulama sürekliliğinin olmayışını, uygulanmayan mantıksal erişim kontrollerini, yazılım ve donanım kurulumunu ve politikayı takip etmeyen değişiklikleri ve var olmayan bir felaket kurtarma planını içerebilir.

Bu güvenlik açığı kaynaklarının üçü de bir ağı veya cihazı kötü niyetli kod saldırıları ve ağ saldırıları dahil olmak üzere çeşitli saldırılara açık bırakabilir.

Fiziksel Güvenlik

Ağ kaynakları fiziksel olarak tehlikeye atılabiliyorsa, bir tehdit aktörü ağ kaynaklarının kullanımını reddedebilir. Dört fiziksel tehdit sınıfı aşağıdaki gibidir:

- **Donanım tehditleri -** Bu, sunuculara, yönlendiricilere, anahtarlara, kablolama tesisine ve iş istasyonlarına fiziksel hasarı içerir.
- **Çevresel tehditler -** Bu, aşırı sıcaklıkları (çok sıcak veya çok soğuk) veya aşırı nemi (çok ıslak veya çok kuru) içerir.
- **Elektriksel tehditler -** Buna voltaj yükselmeleri, yetersiz besleme voltajı (elektrik kesintileri), koşulsuz güç (gürültü) ve toplam güç kaybı dahildir.
- **Bakım tehditleri -** Bu, temel elektrik bileşenlerinin kötü kullanımı (elektrostatik deşarj), kritik yedek parça eksikliği, zayıf kablo bağlantısı ve kötü etiketlemeyi içerir.

Bu sorunları gidermek için iyi bir fiziksel güvenlik planı oluşturulmalı ve uygulanmalıdır.

16.2 Ağ Saldırıları

Kötü Amaçlı Yazılım Türleri

Ağ kaynakları fiziksel olarak tehlikeye atılabiliyorsa, bir tehdit aktörü ağ kaynaklarının kullanımını reddedebilir. Dört fiziksel tehdit sınıfı aşağıdaki gibidir:

- **Donanım tehditleri -** Bu, sunuculara, yönlendiricilere, anahtarlara, kablolama tesisine ve iş istasyonlarına fiziksel hasarı içerir.
- **Çevresel tehditler -** Bu, aşırı sıcaklıkları (çok sıcak veya çok soğuk) veya aşırı nemi (çok ıslak veya çok kuru) içerir.
- **Elektriksel tehditler -** Buna voltaj yükselmeleri, yetersiz besleme voltajı (elektrik kesintileri), koşulsuz güç (gürültü) ve toplam güç kaybı dahildir.
- **Bakım tehditleri -** Bu, temel elektrik bileşenlerinin kötü kullanımı (elektrostatik deşarj), kritik yedek parça eksikliği, zayıf kablo bağlantısı ve kötü etiketlemeyi içerir.

Bu sorunları gidermek için iyi bir fiziksel güvenlik planı oluşturulmalı ve uygulanmalıdır.

Keşif Saldırıları

Kötü amaçlı kod saldırılarına ek olarak, ağların çeşitli ağ saldırılarına da kurban gitmesi mümkündür. Ağ saldırıları üç ana kategoriye ayrılabilir:

- **Keşif saldırıları** - Sistemlerin, hizmetlerin veya güvenlik açıklarının keşfedilmesi ve haritalanması.
- **Erişim saldırıları** - Verilerin, sistem erişiminin veya kullanıcı ayrıcalıklarının yetkisiz manipülasyonu.
- **Hizmet reddi** - Ağların, sistemlerin veya hizmetlerin devre dışı bırakılması veya bozulması.

Keşif saldırıları için, dış tehdit aktörleri, belirli bir şirket veya varlığa atanan IP adres alanını kolayca belirlemek için **nslookup** ve **whois** yardımcı programları gibi internet araçlarını kullanabilir . IP adresi alanı belirlendikten sonra, bir tehdit aktörü, aktif olan adresleri belirlemek için herkese açık IP adreslerine ping atabilir.

Erişim Saldırıları

Erişim saldırıları, web hesaplarına, gizli veritabanlarına ve diğer hassas bilgilere giriş sağlamak için kimlik doğrulama hizmetlerindeki, FTP hizmetlerinde ve web hizmetlerindeki bilinen güvenlik açıklarından yararlanır.

Erişim saldırıları dört türe ayrılabilir:

- **Parola saldırıları -** Kaba kuvvet, truva atı ve paket algılayıcılar kullanılarak gerçekleştirilir
- **Güven istismarı -** Bir tehdit aktörü, bir sisteme erişmek için yetkisiz ayrıcalıkları kullanır ve muhtemelen hedefi tehlikeye atar.
- **Bağlantı noktası yeniden yönlendirme** : - Bir tehdit aktörü, diğer hedeflere yönelik saldırılar için bir üs olarak güvenliği ihlal edilmiş bir sistemi kullanır. Örneğin, güvenliği ihlal edilmiş bir A ana bilgisayarına bağlanmak için SSH'yi (bağlantı noktası 22) kullanan bir tehdit aktörü, ana bilgisayar B'ye güvenir ve bu nedenle tehdit aktörü, ona erişmek için Telnet (bağlantı noktası 23) kullanabilir.
- **Ortadaki Adam -** Tehdit aktörü, iki taraf arasında geçen verileri okumak veya değiştirmek için iki meşru varlık arasında konumlandırılır.

Hizmet Reddi Saldırıları

Hizmet reddi (DoS) saldırıları, en çok duyurulan ve ortadan kaldırılması en zor olan saldırı türüdür. Ancak, uygulama kolaylıkları ve potansiyel olarak önemli hasarları nedeniyle DoS saldırıları, güvenlik yöneticilerinin özel ilgisini hak eder.

- DoS saldırıları birçok biçimde olabilir. Sonuçta yetkili kişilerin sistem kaynaklarını tüketerek bir hizmeti kullanmasını engellerler. DoS saldırılarını önlemeye yardımcı olmak için, işletim sistemleri ve uygulamalar için en son güvenlik güncellemelerini takip etmek önemlidir.
- DoS saldırıları, iletişimi kesintiye uğrattığı ve önemli zaman ve para kaybına neden olduğu için büyük bir risktir. Bu saldırıların, vasıfsız bir tehdit aktörü tarafından bile yürütülmesi nispeten kolaydır.
- DDoS, DoS saldırısına benzer, ancak birden çok, koordineli kaynaklardan kaynaklanır. Örneğin, bir tehdit aktörü, zombiler olarak bilinen virüslü ana bilgisayarlardan oluşan bir ağ oluşturur. Bir zombi ağına botnet denir. Tehdit aktörü, zombilerin botnet'ine DDoS saldırısı gerçekleştirme talimatı vermek için bir komut ve kontrol (CnC) programı kullanır.

Lab – Araştırma Ağı Güvenliği Tehditleri

Bu laboratuvarda aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: SANS Web Sitesini Keşfedin
- Bölüm 2: Son Ağ Güvenliği Tehditlerini Belirleyin
- Bölüm 3: Belirli Bir Ağ Güvenlik Tehdidini Ayrıntılandırın

16.3 Ağ Saldırısının Azaltılması

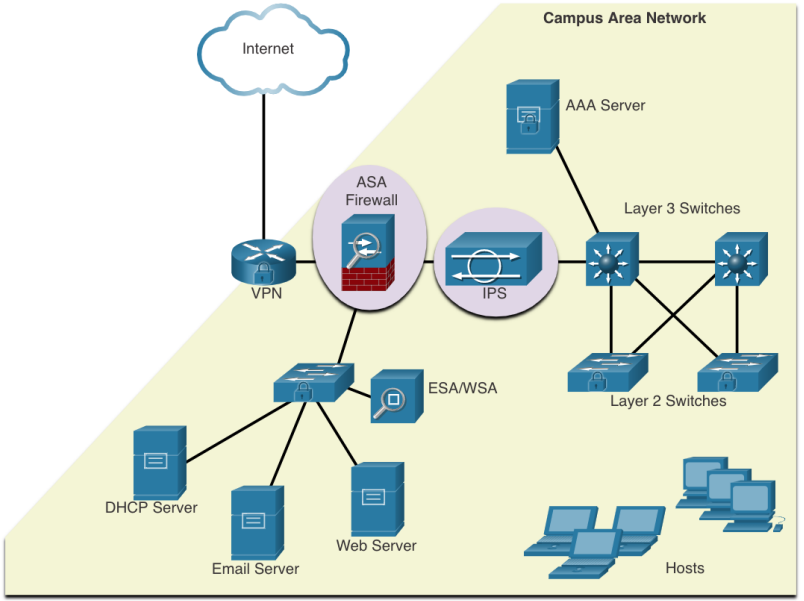
Ağ Saldırısının Azaltılması

Derinlemesine Savunma Yaklaşımı

Ağ saldırılarını azaltmak için önce yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil cihazları güvenli hale getirmelisiniz. Çoğu kuruluş, güvenlik için derinlemesine savunma yaklaşımı (katmanlı yaklaşım olarak da bilinir) kullanır. Bu, birlikte çalışan ağ aygıtları ve hizmetlerinin bir kombinasyonunu gerektirir.

Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için çeşitli güvenlik cihazları ve hizmetleri uygulanır:

- VPN
- ASA Güvenlik Duvarı
- IPS
- ESA / WSA
- AAA Sunucusu



Yedek Tutma

Aygıt yapılandırmalarını ve verileri yedeklemek, veri kaybına karşı korumanın en etkili yollarından biridir. Yedeklemeler, güvenlik politikasında belirtildiği gibi düzenli olarak yapılmalıdır. Veri yedeklemeleri, ana tesise herhangi bir şey olması durumunda yedekleme ortamını korumak için genellikle iş yeri dışında depolanır.

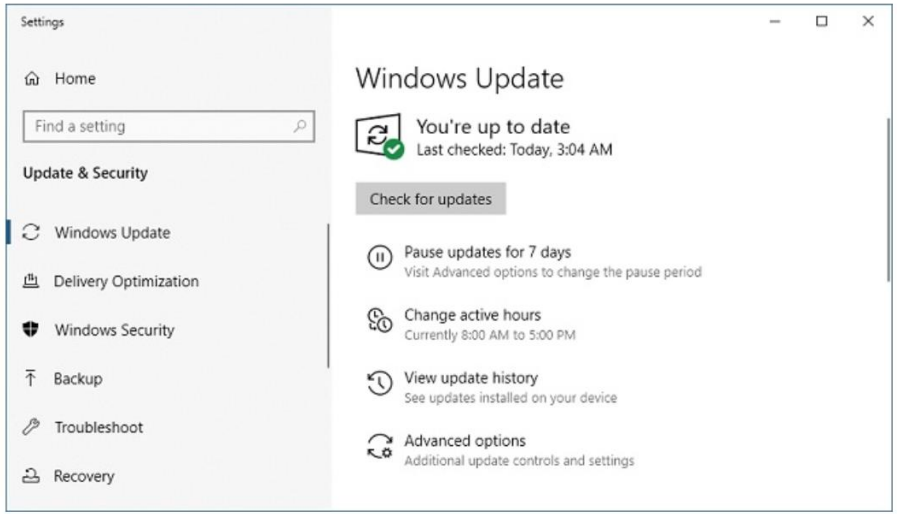
Tablo, yedeklemeyle ilgili konuları ve açıklamalarını gösterir.

Düşünce	Açıklama
Sıklık	• Güvenlik politikasında belirtildiği gibi, düzenli olarak yedekleme yapın. • Tam yedeklemeler zaman alıcı olabilir, bu nedenle değiştirilen dosyaların sık sık kısmi yedeklenmesiyle aylık veya haftalık yedeklemeler gerçekleştirin.
Depolama	• Verilerin bütünlüğünü sağlamak ve dosya geri yükleme prosedürlerini doğrulamak için her zaman yedekleri doğrulayın.
Güvenlik	• Yedekler, güvenlik politikasının gerektirdiği şekilde günlük, haftalık veya aylık rotasyonla onaylanmış bir saha dışı depolama konumuna taşınmalıdır.
Doğrulama	• Yedeklemeler güçlü parolalar kullanılarak korunmalıdır. Verileri geri yüklemek için parola gereklidir.

Yükseltme, Güncelleme ve Yama

Yeni kötü amaçlı yazılım piyasaya sürüldüğünde, işletmelerin antivirüs yazılımının en son sürümlerini güncel tutması gerekir.

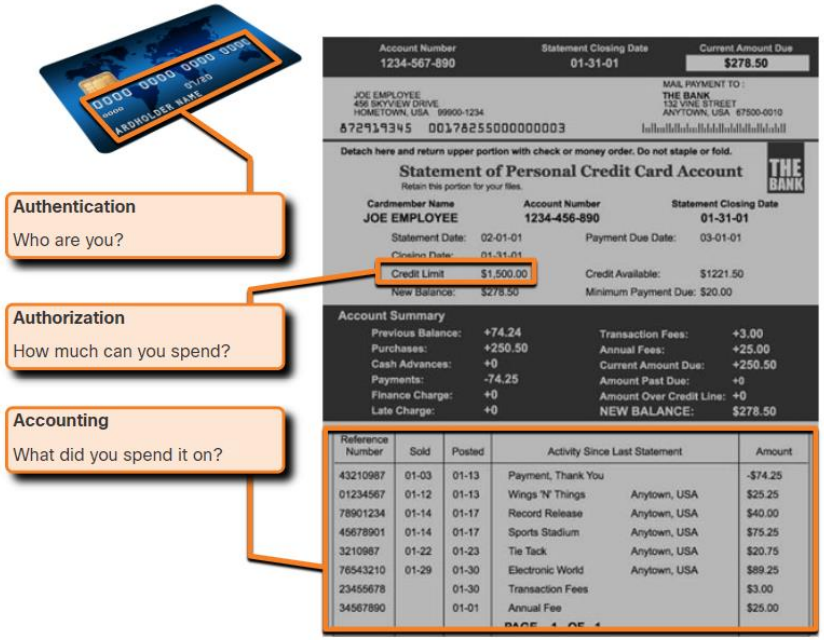
- Bir solucan saldırısını azaltmanın en etkili yolu, işletim sistemi satıcısından güvenlik güncellemelerini indirmek ve tüm savunmasız sistemleri yamamaktır.
- Kritik güvenlik yamalarının yönetimine yönelik bir çözüm, tüm uç sistemlerin güncellemeleri otomatik olarak indirmesini sağlamaktır.



Kimlik Doğrulama, Yetkilendirme ve Hesap Oluşturma

Kimlik doğrulama, yetkilendirme ve hesaplama (AAA veya "üçlü A") ağ güvenliği hizmetleri, ağ cihazlarında erişim denetimini kurmak için birincil çerçeveyi sağlar.

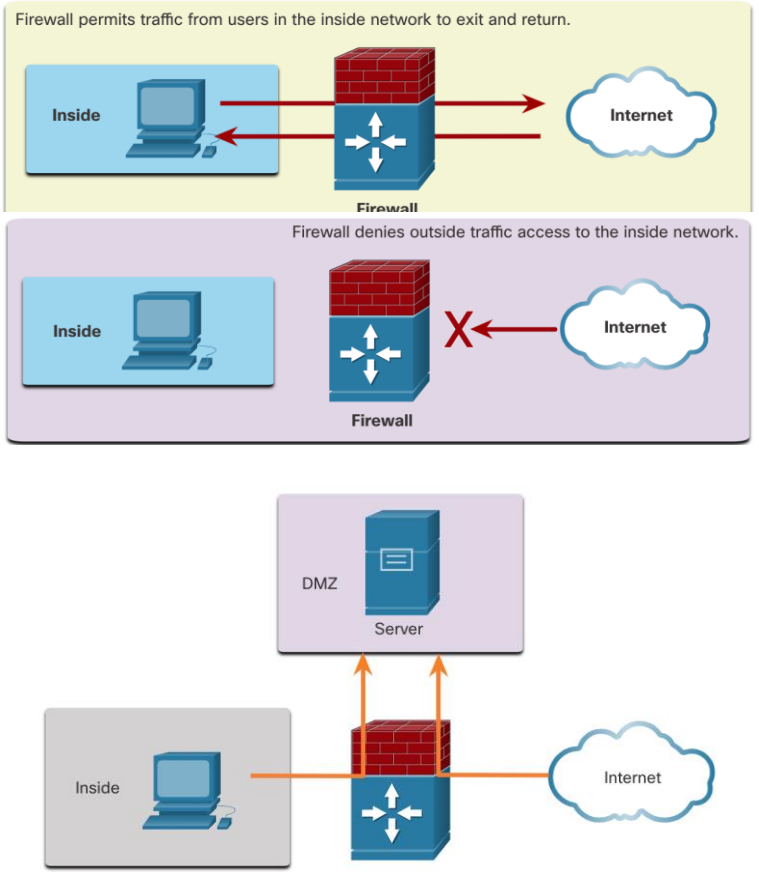
- AAA, bir ağa kimlerin erişmesine izin verildiğini (kimlik doğrulama), ağa erişirken hangi eylemleri gerçekleştirdiklerini (yetkilendirme) ve oradayken yapılanların kaydını tutmanın (hesap oluşturma) bir yoludur.
- AAA kavramı, kredi kartı kullanımına benzer. Kredi kartı, onu kimin kullanabileceğini, bu kullanıcının ne kadar harcayabileceğini tanımlar ve kullanıcının para harcadığı kalemlerin hesabını tutar.



Güvenlik Duvarı

Ağ güvenlik duvarları iki veya daha fazla ağ arasında bulunur, aralarındaki trafiği kontrol eder ve yetkisiz erişimi önlemeye yardımcı olur.

Bir güvenlik duvarı, dış kullanıcıların belirli hizmetlere kontrollü erişime izin verebilir. Örneğin, dış kullanıcılar tarafından erişilebilen sunucular genellikle askerden arındırılmış bölge (DMZ) olarak adlandırılan özel bir ağda bulunur. DMZ, bir ağ yöneticisinin o ağa bağlı ana bilgisayarlar için belirli ilkeler uygulamasını sağlar.



Güvenlik Duvarı Türleri

Güvenlik duvarı ürünleri çeşitli biçimlerde paketlenmiştir. Bu ürünler, bir ağa neyin erişime izin verileceğini veya reddedileceğini belirlemek için farklı teknikler kullanır. Aşağıdakileri içerir:

- **Paket filtreleme** - IP veya MAC adreslerine göre erişimi engeller veya erişime izin verir
- **Uygulama filtreleme** - Bağlantı noktası numaralarına göre belirli uygulama türlerine göre erişimi engeller veya buna izin verir
- **URL filtreleme** - Belirli URL'lere veya anahtar kelimelere göre web sitelerine erişimi engeller veya bunlara izin verir
- **Durum bilgili paket incelemesi (SPI)** - Gelen paketler, dahili ana bilgisayarlardan gelen isteklere verilen meşru yanıtlar olmalıdır. Özel olarak izin verilmedikçe, istenmeyen paketler engellenir. SPI ayrıca hizmet reddi (DoS) gibi belirli saldırı türlerini tanıma ve filtreleme yeteneğini de içerebilir.

Uç Nokta Güvenliği

Bir uç nokta veya ana bilgisayar, bir ağ istemcisi olarak işlev gören bağımsız bir bilgisayar sistemi veya cihazdır. Yaygın uç noktalar dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular, akıllı telefonlar ve tabletlerdir.

Uç nokta cihazlarının güvenliğini sağlamak, insan doğasını içerdiği için bir ağ yöneticisinin en zorlu görevlerinden biridir. Bir şirketin iyi belgelenmiş politikaları olmalıdır ve çalışanlar bu kuralların farkında olmalıdır.

Çalışanların ağın doğru kullanımı konusunda eğitilmesi gerekir. Politikalar genellikle antivirüs yazılımının kullanımını ve ana bilgisayar izinsiz giriş önleme kullanımını içerir. Daha kapsamlı uç nokta güvenlik çözümleri, ağ erişim kontrolüne dayanır.

16.4 Cihaz Güvenliği

Cisco AutoSecure

Bir cihaza yeni bir işletim sistemi yüklendiğinde, güvenlik ayarları varsayılan değerlere ayarlanır. Çoğu durumda, bu güvenlik seviyesi yetersizdir. Cisco yönlendiricileri için, Cisco AutoSecure özelliği sistemin güvenliğini sağlamaya yardımcı olmak için kullanılabilir.

Ek olarak, çoğu işletim sistemi için geçerli olan bazı basit adımlar vardır:

- Varsayılan kullanıcı adları ve şifreler derhal değiştirilmelidir.
- Sistem kaynaklarına erişim, yalnızca bu kaynakları kullanmaya yetkili kişilerle sınırlandırılmalıdır.
- Gereksiz hizmetler ve uygulamalar mümkün olduğunda kapatılmalı ve kaldırılmalıdır.
- Genellikle, üreticiden sevk edilen cihazlar bir süredir bir depoda durmaktadır ve en güncel yama

Şifreler

Ağ cihazlarını korumak için güçlü şifreler kullanmak önemlidir. İşte uyulması gereken standart kurallar:

- En az sekiz karakter uzunluğunda, tercihen 10 veya daha fazla karakter uzunluğunda bir şifre kullanın.
- Parolaları karmaşık hale getirin. İzin veriliyorsa, büyük ve küçük harflerin, sayıların, sembollerin ve boşlukların karışımını ekleyin.
- Tekrarlara, yaygın sözlük kelimelerine, harf veya sayı dizilerine, kullanıcı adlarına, akraba veya evcil hayvan adlarına, doğum tarihleri gibi biyografik bilgilere, kimlik numaralarına, ata adlarına veya diğer kolayca tanımlanabilen bilgilere dayanan şifrelerden kaçının.
- Parolayı kasıtlı olarak yanlış yazın. Örneğin, Smith = Smyth = 5mYth veya Security = 5ecur1ty.
- Parolaları sık sık değiştirin. Bir parola bilinmeden tehlikeye atılırsa, tehdit aktörünün parolayı kullanması için fırsat penceresi sınırlanır.
- Parolaları bir yere yazmayın ve masa veya monitör gibi görünür yerlerde bırakmayın.

Cisco yönlendiricilerinde, parolalar için baştaki boşluklar yok sayılır, ancak ilk karakterden sonraki boşluklar göz ardı edilir. Bu nedenle, güçlü bir parola oluşturmanın bir yolu, boşluk çubuğunu kullanmak ve birçok sözcükten oluşan bir ifade oluşturmaktır. Buna parola denir. Bir parolayı hatırlamak genellikle basit bir paroladan daha kolaydır. Aynı zamanda daha uzun ve tahmin edilmesi daha zor.

Ek Şifre Güvenliği

Parolaların bir Cisco yönlendirici ve anahtar üzerinde gizli kalmasını sağlamaya yardımcı olmak için atılabilecek birkaç adım vardır:

- Tüm düz metin parolalarını **hizmet parolası şifreleme** komutuyla **şifreleyin** .
- **Güvenlik parolaları minimum uzunluk** komutuyla kabul edilebilir bir minimum parola uzunluğu belirleyin .
- İle kaba kuvvet şifre tahmin saldırıları caydırmak **giriş bloğu için # girişimi # içinde #** komutu.
- **Exec-timeout** komutuyla belirli bir süre sonra etkin olmayan ayrıcalıklı bir EXEC modu erişimini devre dışı bırakın .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

SSH'i Etkinleştir

Aşağıdaki adımları kullanarak bir Cisco cihazını SSH'yi destekleyecek şekilde yapılandırmak mümkündür:

Benzersiz bir cihaz ana bilgisayar adı yapılandırın . Bir cihazın varsayılandan farklı bir benzersiz ana bilgisayar adı olmalıdır.

IP alan adını yapılandırın . Genel yapılandırma modu komutu **ip-etki alanı adını** kullanarak ağın IP etki alanı adını yapılandırın .

SSH trafiğini şifrelemek için bir anahtar oluşturun . SSH, kaynak ve hedef arasındaki trafiği şifreler. Bununla birlikte, bunu yapmak için, küresel yapılandırma komutu kullanılarak benzersiz bir kimlik doğrulama anahtarı, **rsa genel anahtar modülü** *bitleri* **oluşturan kripto anahtarı üretilmelidir** . Modül *bitleri* , anahtarın boyutunu belirler ve 360 bit ila 2048 bit arasında yapılandırılabilir. Bit değeri ne kadar büyükse, anahtar o kadar güvenli olur. Ancak, daha büyük bit değerlerinin de bilgileri şifrelemesi ve şifresini çözmesi daha uzun sürer. Önerilen minimum modül uzunluğu 1024 bittir.

Yerel bir veritabanı girişi doğrulayın veya oluşturun . Kullanıcı **adı** genel yapılandırma komutunu kullanarak yerel bir veritabanı kullanıcı adı girişi oluşturun .

Yerel veritabanına göre kimlik doğrulaması yapın . Yerel veritabanına göre vty satırının kimliğini doğrulamak için **oturum açma yerel** hat yapılandırma komutunu kullanın.

Vty gelen SSH oturumlarını etkinleştirin . Varsayılan olarak, vty hatlarında hiçbir giriş oturumuna izin verilmez. **[Ssh | taşıma girdisini** kullanarak Telnet ve SSH dahil olmak üzere birden çok girdi protokolü belirtebilirsiniz. **telnet]** komutu.

Kullanılmayan Hizmetleri Devre Dışı Bırak

Cisco yönlendiricileri ve anahtarları, ağınızda gerekli olabilecek veya olmayabilecek etkin hizmetlerin bir listesiyle başlar. CPU döngüleri ve RAM gibi sistem kaynaklarını korumak için kullanılmayan hizmetleri devre dışı bırakın ve tehdit aktörlerinin bu hizmetleri istismar etmesini önleyin.

Varsayılan olarak açık olan hizmetlerin türü, IOS sürümüne bağlı olarak değişecektir. Örneğin, IOS-XE'de tipik olarak yalnızca HTTPS ve DHCP bağlantı noktaları açık olacaktır. Bunu **show ip ports all** komutu ile doğrulayabilirsiniz .

IOS-XE'den önceki IOS sürümleri show control-plane host open-ports komutunu kullanır.

Paket Tracer –Güvenli Şifreleri ve SSH'yi Yapılandırın

Bu Paket İzleyicide, şifreleri ve SSH'yi yapılandıracaksınız:

- Ağ yöneticisi sizden RTA ve SW1'i dağıtım için hazırlamanızı istedi. Ağa bağlanmadan önce güvenlik önlemlerinin etkinleştirilmesi gerekir.

Lab – Ağ Aygıtlarını SSH ile Yapılandırma

Bu laboratuvarda aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Temel Aygıt Ayarlarını Yapılandırın
- Bölüm 2: Yönlendiriciyi SSH Erişimi için Yapılandırma
- Bölüm 3: Anahtarı SSH Erişimi için Yapılandırma
- Bölüm 4: Anahtardaki CLI'den SSH

16.5 Alıştırmalar ve Sınav

Paket Tracer – Güvenli Ağ Cİhazları

Bu aktivitede, gereksinimler listesine göre bir yönlendirici ve bir anahtar yapılandıracaksınız.

Lab – Güvenli Ağ Cihazları

- Bu laboratuvarda aşağıdaki hedefleri tamamlayacaksınız:
- Temel Cihaz Ayarlarını Yapılandırın
- Yönlendiricide Temel Güvenlik Önlemlerini Yapılandırın
- Anahtarda Temel Güvenlik Önlemlerini Yapılandırın

Bu modülde ne öğrendim ?

- Tehdit aktörü ağa erişim kazandıktan sonra dört tür tehdit ortaya çıkabilir: bilgi hırsızlığı, veri kaybı ve manipülasyon, kimlik hırsızlığı ve hizmet kesintisi.
- Üç temel güvenlik açığı veya zayıflık vardır: teknolojik, yapılandırma ve güvenlik politikası.
- Dört fiziksel tehdit sınıfı şunlardır: donanım, çevre, elektrik ve bakım.
- Kötü amaçlı yazılım, kötü amaçlı yazılımın kısaltmasıdır. Verilere, ana bilgisayarlara veya ağlara zarar vermek, bozmak, çalmak veya "kötü" veya yasadışı eylemde bulunmak için özel olarak tasarlanmış kod veya yazılımdır. Virüsler, solucanlar ve Truva atları kötü amaçlı yazılım türleridir.
- Ağ saldırıları üç ana kategoriye ayrılabilir: keşif, erişim ve hizmet reddi.
- Ağ saldırılarını azaltmak için önce yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil cihazları güvenli hale getirmelisiniz. Çoğu kuruluş, güvenlik için derinlemesine bir savunma yaklaşımı kullanır. Bu, birlikte çalışan ağ aygıtları ve hizmetlerinin bir kombinasyonunu gerektirir.
- Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için çeşitli güvenlik cihazları ve hizmetleri uygulanır: VPN, ASA güvenlik duvarı, IPS, ESA / WSA ve AAA sunucusu.

Bu modülde ne öğrendim ?

- Altyapı cihazlarının, bir FTP veya benzer dosya sunucusunda yapılandırma dosyalarının ve IOS görüntülerinin yedekleri olmalıdır. Bilgisayar veya yönlendirici donanımı arızalanırsa, veriler veya yapılandırma yedek kopya kullanılarak geri yüklenebilir.
- Bir solucan saldırısını azaltmanın en etkili yolu, işletim sistemi satıcısından güvenlik güncellemelerini indirmek ve tüm savunmasız sistemleri yamamaktır. Kritik güvenlik yamalarını yönetmek, tüm uç sistemlerin güncellemeleri otomatik olarak indirdiğinden emin olmak için.
- AAA, bir ağa kimlerin erişmesine izin verildiğini (kimlik doğrulama), oradayken ne yapabileceklerini (yetkilendirme) ve ağa erişirken (hesaplama) hangi eylemleri gerçekleştirdiklerini kontrol etmenin bir yoludur.
- Ağ güvenlik duvarları iki veya daha fazla ağ arasında bulunur, aralarındaki trafiği kontrol eder ve yetkisiz erişimi önlemeye yardımcı olur.
- Uç nokta cihazlarının güvenliğini sağlamak, ağ güvenliği için çok önemlidir. Bir şirketin, antivirüs yazılımının kullanımı ve ana bilgisayar izinsiz giriş önleme gibi iyi belgelenmiş ilkeleri olmalıdır. Daha kapsamlı uç nokta güvenlik çözümleri, ağ erişim kontrolüne dayanır.

Bu modülde ne öğrendim ?

- Cisco yönlendiricileri için, Cisco AutoSecure özelliği sistemin güvenliğini sağlamaya yardımcı olmak için kullanılabilir. Çoğu işletim sistemi için varsayılan kullanıcı adları ve parolalar derhal değiştirilmeli, sistem kaynaklarına erişim yalnızca bu kaynakları kullanma yetkisine sahip kişilerle sınırlandırılmalı ve mümkün olduğunda gereksiz hizmetler ve uygulamalar kapatılmalı ve kaldırılmalıdır.
- Ağ cihazlarını korumak için güçlü şifreler kullanmak önemlidir. Bir parolayı hatırlamak genellikle basit bir paroladan daha kolaydır. Aynı zamanda daha uzun ve tahmin edilmesi daha zor.
- Yönlendiriciler ve anahtarlar için, tüm düz metin parolalarını şifreleyin, minimum kabul edilebilir bir parola uzunluğu belirleyin, kaba kuvvet parola tahmin saldırılarını engelleyin ve belirli bir süre sonra etkin olmayan ayrıcalıklı bir EXEC modu erişimini devre dışı bırakın.
- SSH'yi desteklemek için uygun cihazları yapılandırın ve kullanılmayan hizmetleri devre dışı bırakın.


CISCO